2011

Cracking the Enigma

Mackenzie Smith
University of Redlands

UNIVERSITY OF REDLANDS

Cracking the Enigma

Mackenzie Smith

4/18/2011

Outline

1 Abstract

2 Introduction

3 The Machine: its development and schematics

4 Marian Rejewski

5 Introduction to Permutations

6 Rejewski's Theorem

7 Luck, Math and Mistakes

8 Cracking the Enigma

9 Rejewski's Catalog and Bombe

10 World War II

11 Conclusion

12 References

1 Abstract

This paper will examine the mathematics used to decode the Enigma machine. The Enigma was a machine that was used by the Germans to send secure, encrypted messages amongst each other during World War II. This paper will discuss the workings of the machine and how it was continually adapted to increase security. Polish mathematicians, in particular Marian Rejewski applied theories of permutations of disjoint cycles in order to crack the Enigma cipher. The work done by Rejewski and his colleagues was used by the British at Bletchley Park in order to continue breaking ciphers throughout the war. Being able to read the message sent amongst the German military played a significant role in insuring Ally victory in World War II.

2 Introduction

> *"This is a story about heroes. Its heroes are three Polish mathematicians who in the decade before World War II broke German Enigma messages. It seems rare that mathematicians are heroes of stories, and it seems even rarer that they are heroes because they are mathematicians."*[1]

In the years leading up to and throughout World War II the Germans used a device known as the Enigma Machine to encode and decode confidential messages. The machine was quite complex for its time, having a significant number of initial settings which were changed on a daily basis. The basic cryptanalytic tools of the time could not be used to break the code. However, after many failed attempts in cracking the Enigma, a more advanced method in mathematics was implemented to finally make a breakthrough, having an impact on the outcome of the war.

This paper begins by describing the background information of the events that were occurring at the time, explaining how the Enigma works, along with the basic mathematics of why it was so difficult to break. Then it transitions into how theories on permutations composed of disjoint cycles were used, in particular by Polish mathematician Marian Rejewski, to find patterns in intercepted messages. Once the mathematics of breaking the Enigma code has been covered, the historical impact of this discovery will be discussed.

---

[1] Chris Christensen. "Polish Mathematicians Finding Patterns in Enigma Messages". In *Mathematics Magazine.* Vol. 80, No. 4, October 2007. p.247

3 The Machine: its development and schematics

With the birth of radio transmission, communication from military bases to ships and submarines, as well as communication to other bases, across great distances became achievable in just a matter of seconds. However, a disadvantage to this new technology was that radio transmissions were easily intercepted by the enemy; therefore a ciphering system needed to be implemented in order to keep the messages confidential. The more complex the cipher was, the harder it was to crack, but it also left a lot of room for error. For example, making an error in encoding or decoding just one letter could mean the difference between life and death. Thus individuals from several countries decided that a machine needed to be used for the enciphering and deciphering of messages to eliminate that chance of error.[2]

In 1918, a German electrical engineer by the name of Arthur Scherbius invented a machine that soon would serve a significant role in the upcoming Second World War. He named the machine the "Enigma" in order to promote sales, as it was the Greek word for riddle.[3] A promotion for the machine read:

> *If you have no good coding system, you are always running a considerable risk. Transmitted by cable or without wire, your correspondence will always be exposed to every spy, your letters, to being opened and copied, your intended or settled contracts, your offers and important news to every inquisitive eye. Considering this state of things, it is almost inconceivable that persons interested in those circumstances should delay securing themselves better against such things. Yet, ciphering and deciphering has been a troublesome art hitherto. . . . Now, we can offer you our machine "Enigma", being a universal remedy for all those inconveniences.*[4]

---

[2] Robert Churchhouse. "Codes and Ciphers: Julius Caesar, the Enigma, and the Internet". New York: Cambridge University Press. 2002. p.111
[3] Rudolph Kippenhahn. "Code Breaking: A History and Exploration". New York: The Overlook Press. 1999. p. 160
[4] Christensen p.249

The original machine produced for commercial use consisted of six main components:

a. a 26-letter keyboard for inputting the plaintext
b. 26 lamps representing each letter to indicate the cipher letter
c. a power supply which for the initial machine was a 3.5 volt battery
d. three wired rotors that were interchangeable and were engraved with the letters of the alphabet around their circumferences
e. a fixed wired reflector, which ensured that when using the same settings encoding and decoding were the same
f. a fixed wired entry wheel[5]

Scherbius was an inventor and the inadequacy of cryptographic systems used in World War I inspired him to construct a machine that would help decrease human error, as well as make encoding and decoding more efficient. He was able to accomplish these goals with the automatic movement of each rotor, along with the speed of electricity.[6] The German military became very interested in what the machine could do; thus Scherbius built three new rotors and a new reflector, all with different wirings from those sold commercially, to be used strictly by the German military. By 1925, he began mass-producing the military version of the machine, and throughout this time sold over 30,000 machines to the German military. The changes to the machine ensured that a message encoded with the military machine could not be decoded with the commercial machine. The Enigma provided the German military with the most secure system of cryptography in the world, which at the time they thought would play a vital role in ensuring Nazi victory in World War II. Unfortunately, Scherbius died in 1929 when a carriage he was riding in crashed into a wall, so he was not able to experience the important role his invention would have over the next decade.[7]

---

[5] Churchhouse pg. 112
[6] Simon Singh. "The Code Book: The Evolution of Secrecy from Mary Queen of Scots to Quantum Cryptography". New York: Random House. 1999. pp. 127, 132
[7] Singh p. 142

The wired reflector Scherbius included in the machine was what distinguished the Enigma from other similar machines being invented at the time; it allowed users to use the same machine at the same settings and set-up, for both encipherment and decipherment. While the reflector served as a useful component, it was actually the part of the machine that allowed the British and Polish cryptologists to decode encrypted messages, which will be discussed in greater detail later.[8] Another appealing aspect of the machine was its portability. It was small enough to take onboard submarines and ships, and to have out in the field. Similar machines were used during this time by other countries. The British used a machine known as Type X, the Americans had SIGABA, and the Japanese relied on PURPLE, though none of them were quite like the Enigma.[9]

To encode or decode a message the user would set the machine to the specific initial settings being used for the message. The user would press the first letter of the message on the keyboard, and the enchiphered letter would light up. After each letter was pressed the rotor in the rightmost position would rotate by $1/26^{th}$. The rotation put the machine in a new setting, producing a different monoalphabetic substitution cipher. It is important to note that, before the very first letter of a message was encrypted, the first rotor rotated by $1/26^{th}$ before encipherment. When that first rotor reached a certain position it would cause the second rotor, in the middle position, to rotate by $1/26^{th}$, and would rotate by $1/26^{th}$ every 26^{th} letter thereafter. Similarly the third and leftmost rotor would rotate by $1/26^{th}$ after the second rotor reached a certain position, and would rotate $1/26^{th}$ every 676^{th} letter thereafter. However, the machine was also built in such a way that a rotation of the third rotor would also cause a

[8] Kippenhahn p. 163
[9] Paul Lunde. "The Book of Codes: Understanding the World of Hidden Messages". California: University of California Press. 2009. p.118

rotation of the second rotor. Thus the second rotor moved slightly more frequently than once every 26 letters. With these rotations a different setting would be used:

$$26 * 25 * 26 = 16900$$

times in succession before returning to the initial setting.[10] With 16,900 different substitution ciphers being used in succession, common cryptology methods were useless in any efforts to decode a message.

Now, with all of the components in place, the total number of initial settings can be calculated using basic principles of combinatorics. There are 26 options for the starting position of each of the three rotors:

$$26 * 26 * 26 = 17576$$

But the position of each of the three rotors in the machine were interchangeable; therefore we must multiply by 3!:

$$17576 * 3! = 105456$$

Prior to the invention of computers, 105,456 initial settings would appear to be a daunting enough number to face. However, the Germans wanted to ensure that the Enigma would not be cracked. Therefore, the military version of the Enigma included another component; that of the plugboard, with which the original number of starting positions increased significantly. The plugboard was added in 1928 and consisted of 26 plugs, one for each letter, and six cables (also

[10] Churchhouse p. 119

known as stecks) which would connect two letters. Those connected letters would replace each other when encoding and decoding a message. This addition of the plugboard consisted of:

$$\frac{\binom{26}{2}\binom{24}{2}\binom{22}{2}\binom{20}{2}\binom{18}{2}\binom{16}{2}}{6!} = 1.00391795\text{x}10^{11}$$

different settings, which increased the total number of initial settings to:

$$105456 * 1.00391795\text{x}10^{11} = 1.058691676\text{x}10^{16}$$

In a sales brochure for the commercial machine, manufacturers aimed to intrigue customers by advertising the machine's security:

> *[If] a man were able to adjust, day and night, a new key at every minute, it would take him 4000 years to try all those possibilities through on[e] after another.*[11]

After British and Polish cryptologists, mathematicians and linguists had been working on cracking the Enigma, the Germans made the machine even more secure. In 1938 two more rotors were introduced, thus allowing the user to now choose three of the five total rotors to encode a message. As if that were not enough, a month later they also increased the number of cables used on the plugboard from six to ten.[12] Therefore, with these new elements, the number of initial settings increased yet again.

The addition of the two new rotors gave a total of:

$$26^3 * \binom{5}{3} * 3! = 1{,}054{,}560$$

rotor settings.

The addition of the four extra cables increased the number of plugboard settings to:

$$\frac{\binom{26}{2}\binom{24}{2}\binom{22}{2}\binom{20}{2}\binom{18}{2}\binom{16}{2}\binom{14}{2}\binom{12}{2}\binom{10}{2}\binom{8}{2}}{10!} = 1.507382749\text{x}10^{14}$$

---

[11] Christensen p. 253
[12] Singh p. 157

This resulted in:

$$1054560 * 1.507382749\text{x}10^{14} = 1.589625552\text{x}10^{20}$$

initial settings for the new, more secure version of the Enigma.

The Germans used these calculations to determine the security of the Enigma; however, in doing so they made some assumptions about what their enemy might know. Their main assumption was that the Allies knew the wirings of each rotor, which was a fair assumption since over 30,000 machines were spread throughout the German military. If one were to try to crack the Enigma with absolutely no information about the wirings, the total number of possible settings would be over 10^{87}, because you would then incorporate all of the possible ways each rotor could connect all 26 letters. [13]

Consider an 8-letter Enigma as shown below. Let *R* represent the reflector, *L* be the third rotor, *M* be the middle rotor, *N* be the first rotor and *S* be the switchboard. To encrypt the letter D the following would occur:

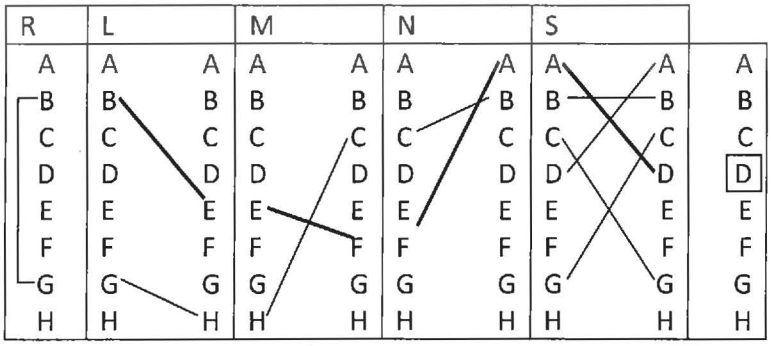


Figure 3.1

Assuming that the first rotor has already made its initial rotation, when the key D is pressed the current enters the switchboard where D is connected to A. In the first rotor *N,* A is connected to

[13] Churchhouse p. 120

F; then in rotor *M*, F is wired to E; and in rotor L, E is wired to B. At this point the current now enters the reflector, *R*:

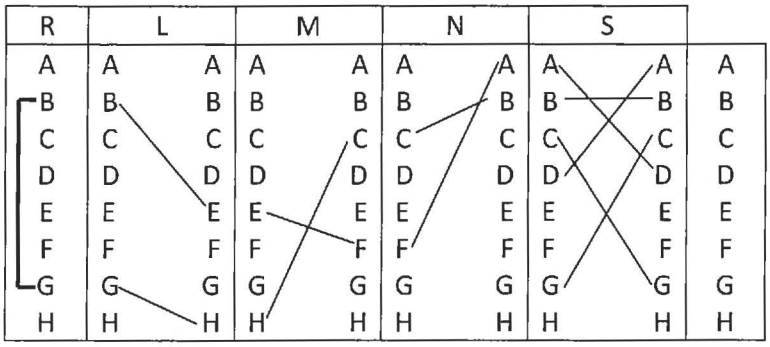


Figure 3.2

In the reflector B is wired to G, so the current will pass back through the machine starting at the letter G as follows:

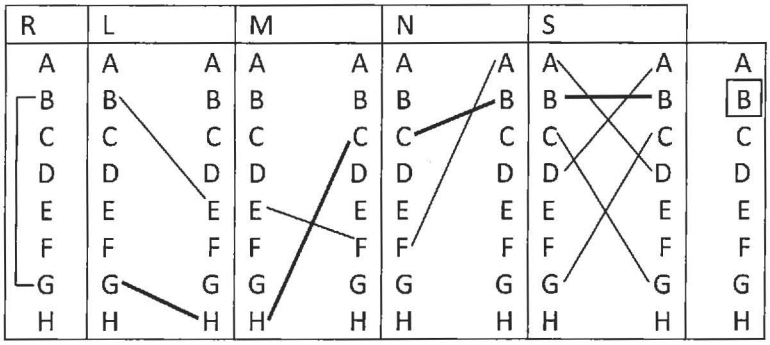


Figure 3.3

Going back through the machine, G is wired to H in rotor *L*; H is wired to C in rotor *M*; and in rotor *N*, C is wired to B. In the switchboard, B is not swapped with another letter; therefore the light bulb under the letter B will light up, and this 8-letter Enigma at the setting AAH, encrypts D to B (recall, the machine set at AAH will rotate to the setting AAA before encrypting the letter). The reflector allows for the process of encryption and decryption to be the same, so looking at the wirings in the above Enigma, pressing the letter B would follow the reverse path as the

encryption of D. Therefore, at that setting, B is encrypted as D. After D is encrypted, rotor *N* will rotate one position as follows:

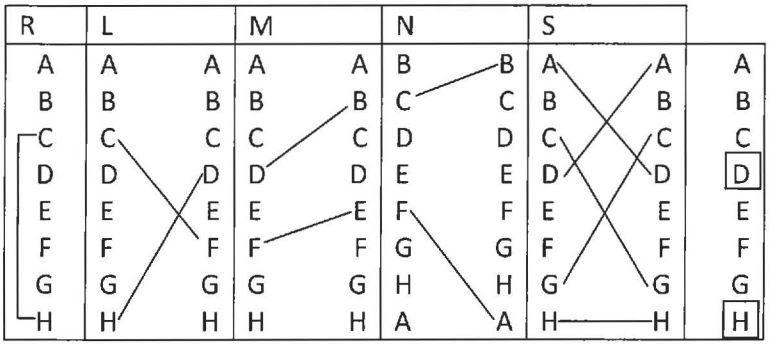


Figure 3.4

Following the encryption of D through the machine, D now is encrypted as H at the setting AAA, and rotor *N* would again rotate for the encryption of the next letter.

4 Marian Rejewski

The Poles' interest in the Enigma was sparked at the beginning of 1928, when a parcel arrived at the customs house in Warsaw. Claiming it contained radio equipment, German government officials insisted that customs turn over the parcel to them immediately. Noticing their urgency, the Polish customs officers became suspicious, and claimed that the parcel had not arrived yet. The customs officers informed the Cipher Bureau; a department of the government that had an interest in radio equipment. After carefully opening the box, it was determined the contents were that of the commercial version of the Enigma machine, for the military version had not been built yet. The machine and its inner workings were thoroughly examined before the parcel was carefully resealed. This discovery prompted the Poles to

purchase a commercial Enigma to further investigate how it was used to encode and decode messages.[14]

Throughout its history, Poland had developed a department of their government known as Biuro Szyfrów, or the Cipher Bureau. As stated by Simon Singh, author of *The Code Book,* "For centuries, it had been assumed that the best cryptanalysts were experts in the structure of language, but the arrival of the Enigma prompted the Poles to alter their recruiting policy."[15] Since the machine was mechanical, it was thought that a more scientific mind would have a better understanding of the inner workings of the Enigma and thus a better chance of cracking it. Therefore, towards the end of 1928, the Bureau organized a course in cryptography and invited twenty mathematicians from the university at Poznán to participate.[16] While Poznán was not the most respected school in Poland, it was located in the western part of the country, which up until 1918 was part of Germany; therefore, its students were fluent in German. During these courses in cryptography, three students in particular stood out and were recruited into the Bureau in 1932.[17]

The three mathematicians chosen were, Henryk Zygalski, Jerzy Różycki and Marian Rejewski. Of the three, Rejewski was the most gifted; at the age of twenty-three he had been studying statistics to pursue a career in insurance when this opportunity came to him. Rejewski was born on August 16, 1905, in Bydgoszcz, Poland. He studied mathematics while earning a Master of Philosophy from the University of Poznán.[18] After successfully decoding a number of traditional ciphers, he was confronted with the Enigma. He worked completely on his own and

---

[14] Marian Rejewski. "How Polish Mathematicians Deciphered the Enigma". In *Annals of the History of Computing.* Vol. 3, Number 3, July 1981. Florida. 1981. p.213
[15] Singh p.149
[16] Rejewski p. 214
[17] Singh p.149
[18] Rejewski p. 214

began to break down the individual components of the machine. Simon Singh described Rejewski's work as follows: "as with all mathematics, his work required inspiration as well as logic." Another wartime cryptanalyst with a background in mathematics expanded on Singh's description, claiming, "the creative codebreaker must perforce commune daily with dark spirits to accomplish his feats of mental ju-jitsu'."[19] After being assigned to the Enigma, Rejewski soon realized, just as the Bureau had, that his experience in mathematics would be much more useful than familiarity with the German language.

5 Introduction to Permutations

Before we begin to discuss the mathematics behind decoding the Enigma, it is important to understand the terminology and notation, and to be aware of certain theorems.

DEFINITION 5.1 A function from *A* to *B* is **one-to-one** if each element of *B* has at most one element of *A* mapped to it; that is, if $f(a) = f(b)$, then a always equals b.[20]

DEFINITION 5.2 A function from *A* to *B* is **onto** if each element of *B* has at least one element of *A* mapped to it.[21]

DEFINITION 5.3 A **permutation** of a set *A* is a function from *A* to *A* that is both one-to-one and onto.[22]

A permutation has matrix-like notation; for example, given the mapping α:{1,2,3,4}→{1,2,3,4}, such that $\alpha(1)=3$, $\alpha(2)=1$, $\alpha(3)=4$, and $\alpha(4)=2$, the permutation would be written as:

$$\alpha = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 4 & 2 \end{bmatrix}$$

---

[19] Singh p.149
[20] John Fraleigh. "A First Course in Abstract Algebra". Massachusetts: Addison-Wesley Publishing Company. 1967. p.33
[21] Fraleigh p.33
[22] Joseph Gallian. "Contemporary Abstract Algebra". 5th ed. New York: Houghton Mifflin Company. 2002. p.93

where $\alpha(n)$ is written directly below n.

Permutations can undergo common operations, such as taking the composition of two functions. For example:

Given

$$\alpha = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 4 & 2 \end{bmatrix} \text{ and } \beta = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 1 & 2 \end{bmatrix}$$

$$\alpha\beta = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 3 & 1 \end{bmatrix}$$

When composing two permutations you compute right to left, so using the example above when computing $\alpha\beta(1)$, you find $\beta(1)$, which in the example equals 4, then take $\alpha(4)$, which equals 2; thus $\alpha\beta(1) = 2$. The rest of $\alpha\beta$ is computed the same way. Since calculating the product of two permutations is the same as composing two functions, $(\alpha\beta)(1)=(\alpha(\beta(1))$.

It is important to note that the composition of two permutations is not commutative; that is, $\alpha\beta \neq \beta\alpha$. Using our above example:

$$\beta\alpha = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 2 & 3 \end{bmatrix} \neq \begin{bmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 3 & 1 \end{bmatrix} = \alpha\beta$$

A power of a permutation can also be computed; for example:

$$\alpha^2 = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{bmatrix}$$

The second power of a permutation is the composition of the function with itself, so $\alpha^2(1) = \alpha(\alpha(1))$ is computed by finding $\alpha(1)$, which equals 3, then $\alpha(3)$, which equals 4. Thus $\alpha^2(1) = \alpha\big(\alpha(1)\big) = 4$.

Permutations are one-to-one and onto functions; therefore an inverse function exists.

DEFINTION 5.4 The **inverse** is defined for all $n \in A$, with $\alpha^{-1}(n) = m$ if and only if $\alpha(m) = n$.

Thus:

$$\alpha^{-1} = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 1 & 3 \end{bmatrix}$$

DEFINITION 5.5 The **identity permutation** ι, is the permutation such that $\iota(k) = k$, for all k in A.[23] For our example, this would be written as:

$$\iota = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{bmatrix}$$

DEFINITION 5.6 A **cycle of length k**, denoted $(a_1, a_2, \ldots, a_k)$, is a permutation that maps each element to the one following it, except the last one, which is mapped to the first element; thus $a_1 \rightarrow a_2 \rightarrow \ldots \rightarrow a_k \rightarrow a_1$.[24] Or $\begin{bmatrix} a_1 & a_2 \ldots a_{k-1} & a_k \\ a_2 & a_3 \ldots a_k & a_1 \end{bmatrix}$

When writing the permutation:

$$\alpha = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 4 & 2 \end{bmatrix}$$

in cycle notation, it would be written as $\alpha = (1342)$.

DEFINITION 5.7 Two or more cycles are **disjoint** if there is no element that appears in more than one cycle.

THEOREM 5.1: Every permutation of a finite set can be written as a cycle or as a product of disjoint cycles.

For example:

$$\alpha = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 1 & 2 & 4 \end{bmatrix}$$

---

[23] Marlow Anderson; Todd Feil. "A First Course in Abstract Algebra: Rings, Groups, and Fields". 2nd ed. Florida: Chapman and Hall Press. 2005. p.380

[24] Fraleigh p. 40

can be written as (13)(254).

Proof: Let α be a permutation of a finite set *S* of elements. Let $a_1 \in S$, with $\alpha(a_1) = a_2$, $\alpha(a_2) = \alpha\big(\alpha(a_1)\big) = a_3 = \alpha^2(a_1)$ and so on until $\alpha^m(a_1) = a_1$ for some positive integer m to get the cycle $(a_1, a_2, \dots, a_m)$. We show m exists as follows: S is a finite set which implies that $\alpha^k(a_i) = a_i$ for some positive integers *k* and *i*. Therefore, since $(a_1, a_2, \dots, a_m)$ is a cycle there exist some positive integers *k* and *l* such that $\alpha^k(a_1) = a_1 = \alpha^l(a_1)$ where $l > k$ and $l - k$ is smallest. Since α is one-to-one and onto, it has an inverse function α^{-1}; therefore $a_1 = \iota(a_1) = \alpha^{-k}\Big(\alpha^k(a_1)\Big) = \alpha^{-k}\Big(\alpha^l(a_1)\Big) = \alpha^{l-k}(a_1)$. Thus, by letting *m=l-k*, $\alpha^m(a_1) = \alpha(a_m) = a_1$. Therefore, we have constructed the cycle $(a_1, a_2, \dots, a_m)$. If all elements of S are in the cycle, then we are done and α is a cycle of length m. However, if α does not contain all elements of S, we must find another cycle. Similar to how we constructed $(a_1, a_2, \dots, a_m)$, we will find a cycle $(b_1, b_2, \dots, b_t)$ by choosing an element b_1 of S that is not in $(a_1, a_2, \dots, a_m)$. Let $\alpha(b_1) = b_2, \alpha(b_2) = \alpha\big(\alpha(b_1)\big) = b_3 = \alpha^2(b_1)$ and so on until $\alpha^t(b_1) = b_1$. We know that no element of $(a_1, a_2, \dots, a_m)$ will be in $(b_1, b_2, \dots, b_t)$, because if $\alpha^i(a_1) = \alpha^j(b_1)$ for some positive integers i and j, for which, without loss of generality, $i \geq j$, then $\alpha^{i-j}(a_1) = b_1$ for $i - j \geq 0$. This means b_1 would equal some element of $(a_1, a_2, \dots, a_m)$, contradicting how b_1 was chosen. Thus $(a_1, a_2, \dots, a_m)(b_1, b_2, \dots, b_t)$ is a product of disjoint cycles. If all elements of S are in this product of cycles, then we are done; otherwise, the process above is repeated beginning with an element of S that is not found in any of the previously constructed cycles, until all elements of S are exhausted. We know this will occur because S is finite, and the permutation α is written as a product of disjoint cycles. Therefore, every permutation of a finite set can be written as a cycle or a product of disjoint cycles.

Another important characteristic of permutations that will be used later is the fact that the conjugation of a permutation preserves its cycle structure. While products of permutations are commonly composed today from right to left, for the rest of this paper permutations will be applied left to right as that is how Rejewski carried out his work.

DEFINTION 5.8 Given a group G with $g, h \in G$, we call the element $g^{-1}hg$ the **conjugate** of h by g.[25]

THEOREM 5.2 Conjugation of permutation preserves disjoint cycle structure. That is, if we express permutation α as a product of m disjoint cycles of lengths $k_1, k_2, \dots, k_m$, then any conjugate of α can be expressed as a product of m disjoint cycles, of lengths $k_1, k_2, \dots, k_m$.[26]

For example given:

$$\alpha = (15)(236)(47) \text{ and } \beta = (2531)(647)$$

The conjugate of α by β is:

$$\beta^{-1}\alpha\beta = (23)(145)(67)$$

Thus the disjoint cycle structure of α is preserved.

It is useful to note that when applying the permutation β to the elements of each disjoint cycle in α it is seen that given some element x in a disjoint cycle of length t in α, $\beta(x)$ is an element of a disjoint cycle of length t in $\beta^{-1}\alpha\beta$. That is given:

$$\alpha = (15)(236)(47) \quad \beta = (2531)(647) \text{ and } \beta^{-1}\alpha\beta = (145)(23)(67)$$

$$\beta(1) = 2, \beta(5) = 3$$

[25] Anderson and Feil p. 439
[26] Anderson and Feil p. 439

The elements 1 and 5 compose a cycle of length two in α, and the elements $\beta(1) = 2, \beta(5) = 3$ compose a cycle of length two in $\beta^{-1}\alpha\beta$. Similarly for the cycle of length three in α, (236), after applying β:

$$\beta(2) = 5, \beta(3) = 1 \text{ and } \beta(6) = 4.$$

We get the cycle of length three in $\beta^{-1}\alpha\beta$, (145). And from the other cycle of length two in α, (47):

$$\beta(4) = 7 \text{ and } \beta(7) = 6$$

(67) being the last cycle of length two in $\beta^{-1}\alpha\beta$.

Proof of Theorem 5.2: Let α and β be two permutations of degree k. We want to show given $\alpha = (a_1, a_2, \dots, a_k)$, then $\beta^{-1}\alpha\beta = \big(\beta(a_1), \beta(a_2), \dots, \beta(a_k)\big)$. That is if $\alpha(a_1) = a_2$, then under the permutation $\beta^{-1}\alpha\beta$, $\beta(a_1) \to \beta(a_2)$.

The permutation $\beta^{-1}\alpha\beta$ as a function must be applied right to left; therefore to convert the permutations to a function we must use the standard function notation and write the function as $\beta \bullet \alpha \bullet \beta^{-1}$. Consider $\beta(a_i)$. $\beta \bullet \alpha \bullet \beta^{-1}(\beta(a_i)) = \beta \bullet \alpha(a_i) = \beta(a_{i+1})$ for all $i = (1,2, \dots, k-1)$ since $\alpha(a_i) = a_{i+1}$; therefore $\beta(a_i) \to \beta(a_{i+1})$. Now consider $\beta(a_k)$. $\beta \bullet \alpha \bullet \beta^{-1}(\beta(a_k)) = \beta \bullet \alpha(a_k) = \beta(a_1)$. Thus given $\alpha = (a_1, a_2, \dots, a_k)$, then $\beta^{-1}\alpha\beta = \big(\beta(a_1), \beta(a_2), \dots, \beta(a_k)\big)$. Therefore cycle structure is preserved.

Some other properties of conjugation will become useful as we work through the mathematics of cracking the Enigma, such as:

COROLLARY 5.1 Given two permutations A and B both of degree n, containing only disjoint cycles, with $A = K^{-1}BK$, we can find finitely many possible solutions for K where K must be of the following form:

$$K = \begin{bmatrix} b_1 & b_2 & , \dots, & b_n \\ a_i & a_{i+1}, & \dots, & a_{i-1} \end{bmatrix}$$

For some positive integers n and i. Where the number of solutions found is dependent on the number and lengths of the disjoint cycles in A and B.

Proof: From Theorem 5.2 we know $A = (a_1, a_2, \dots, a_n) = (K(b_1), K(b_2), \dots, K(b_n)) = K^{-1}BK$, where $(b_1, b_2, \dots, b_n)$ correspond to the elements in A. Therefore if $K(b_1) = a_i$ then from the proof of Theorem 5.2 $K(b_2) = a_{i+1}$. Thus given $A = K^{-1}BK$:

$$K = \begin{pmatrix} b_1 & b_2 & , \dots, & b_n \\ a_i & a_{i+1}, & \dots, & a_{i-1} \end{pmatrix}$$

Therefore, by letting i be such that, $1 \leq i \leq n$, we can find n possible solutions for K.

6 Rejewski's Theorem

DEFINITION 6.1 A cyclic permutation of length 2 is known as a **transposition.**

As stated earlier, while the reflecting drum made encoding and decoding Enigma messages easier and possible with the same machine, it also turned out to be a component of the machine that helped enable the Allies to crack the Enigma. The reflector made it so that, given a specific initial setting, if pressing the letter r made the lamp under d light up, then, at that same setting, pressing d would cause r to light up. Therefore, at that setting r→d and d→r, giving the transposition (dr). Such transpositions could be written for the entire alphabet at a given setting. In fact, we will see that at each setting of the Enigma there is a monoalphabetic substitution cipher that can be written as a permutation consisting of 13 disjoint transpositions.

DEFINTION 6.2 Given a set S with *n* elements, a permutation α of the set S is said to be of **degree** *n.*

The following theorem is said to be Rejewski's Theorem, for this property of permutations led him to finding patterns in the machine, which ultimately led to his success in cracking the Enigma.

THEOREM 6.1: Given two permutations are of degree $2n$, so that each consists only of disjoint transpositions, then their product contains an even number of disjoint cycles of each length.

For example, given the permutations:

$$A = (ah)(be)(cf)(ji)(gl)(kd) \text{ and } B = (ac)(bf)(dl)(eh)(gk)(ij)$$

$$AB = (aef)(bhc)(dg)(i)(j)(kl)$$

The product *AB* consists of six disjoint cycles; two cycles of length three, two cycles of length two and two cycles of length one; thus, an even numbers of disjoint cycles of the same lengths.

Proof: Let *S* be a set of 2*n* elements. Let *A* and *B* be two permutations of *S,* each of which is composed only of disjoint transpositions. Choose an element in *S*, say a_1, which is mapped to the element a_2 by *A.* That same element a_2 of *S* is mapped to some element, a_3, by the permutation *B.* Then that element a_3 is mapped to some element a_4 by *A,* which is then mapped to some a_5 by *B.* Given this information, we can write some or all of *A* and *B* as:

$$A=(a_1, a_2)(a_3, a_4)\ldots(a_{2k-1}, a_{2k})\ldots$$

$$B=(a_2, a_3)(a_4, a_5)\ldots(a_{2k}, a_1)\ldots$$

for some positive integer *k* such that $k \leq n$. We know some element a_{2k} will be mapped to a_1 by *B,* because permutations are onto functions.

When computing the product of *A* and *B* we get:

$$AB=(a_1, a_3,\ldots, a_{2k-3}, a_{2k-1})(a_{2k}, a_{2k-2},\ldots, a_4, a_2)\ldots$$

Thus the product *AB* is composed of an even number, namely 2, of disjoint cycles of length *k*. If all 2*n* elements of *S* were exhausted, we are done. Otherwise, the same process as above is followed to find two more cycles of even length. We find these cycles by choosing some b_1 in *S* that is not in $(a_1, a_2)(a_3, a_4)\ldots(a_{2k-1}, a_{2k})$. Then use that element b_1 to find another fragment of the permutation $A= (b_1, b_2)(b_3, b_4)\ldots(b_{2m-1}, b_{2m})\ldots$ and the corresponding fragment of *B* represented by $(b_2, b_3)(b_4, b_5)\ldots(b_{2m}, b_1)\ldots$, where $1 \leq m \leq n - k$. We know $a_i \neq b_j$ for any positive integers $i \leq 2k$ and $j \leq 2m$ because permutations are one-to-one functions, so no two elements will map to the same element in *S*. When we take the composition *AB* with our additional fragments of *A* and *B* we get:

$AB=(a_1, a_3,\ldots, a_{2k-3}, a_{2k-1})(a_{2k}, a_{2k-2},\ldots, a_4, a_2)(b_1, b_3,\ldots, b_{2m-3}, b_{2m-1})(b_{2m}, b_{2m-2},\ldots, b_4, b_2)\ldots$

We have added two more disjoint cycles of the same length *m*, and thus have maintained an even number of cycles of the same length. This process is repeated until all 2*n* elements of *S* have been used. Therefore, if two permutations of degree $2n$ consist only of disjoint transpositions, then their product contains even numbers of disjoint cycles of the same lengths.

Following theorem 6.1, Rejewski was able to incorporate several other properties of permutations, that were helpful to his work.

THEOREM 6.2 Let *X* and *Y* be two permutations of the same even degree, each consisting only of disjoint transpositions. Let $A = (a_1, a_2, \ldots, a_n)$ be a cycle of length n in the product XY. Then $(a_i x_j)$ is a transposition in X if and only if x_j is an element of a cycle $B = (b_1, b_2, \ldots, b_n)$ of length n in XY, where the cycle B is not equal to A. Then given $(a_i b_j)$, $(a_{i+1} b_{j-1})$ is also a transposition in X.

That is, given a permutation *XY* consisting of an even number of cycles of the same length we can solve for possible solutions for the permutation *X* and the permutation *Y* by matching up elements from cycles of the same lengths.

This will present more than one possible solution for *X* and *Y* for some permutation *XY*; therefore a method used to find all solutions for *X* and *Y* is to take two cycles of the same length and write the inverse of one beneath the other, then proceed to shift the bottom permutation through all possibilities. For example given:

$$XY = (146)(258)(3)(7),$$

we would write the inverse of (258) under (146) and (3) under (7):

$$\begin{matrix}(146) & (7)\\ (852) & (3)\end{matrix}$$

This first position results in *X*=(18)(45)(62)(37) and the corresponding *Y*=(84)(56)(21)(37). We then shift the bottom cycles to the left by one position to get:

$$\begin{matrix}(146) & (7)\\ (528) & (3)\end{matrix}$$

In this next position we arrive at the permutation *X*=(15)(42)(68)(37) and the corresponding *Y*=(54)(26)(81)(37). Shifting the third and final time we get:

$$\begin{matrix}(146) & (7)\\ (285) & (3)\end{matrix}$$

Resulting in *X*=(12)(48)(65)(37) and the corresponding *Y*=(24)(15)(68)(37). Therefore we have three possible solutions for *X* and *Y*.

In order to better understand the proof of Theorem 6.2 it is helpful to examine some examples of how this theorem works. For cycles of length one and two the inverse of the cycle is the same as the original cycle, therefore we want to show that two cycles of length one in *XY*,

contain the same elements that make up a transposition in *X* and *Y*. Similarly the components of cycles of length two in *XY* resulted from transpositions that pair those components.

Consider the permutation $XY = (146)(258)(3)(7)$, we assume X and Y are permutations consisting only of disjoint transpositions, and solve for their possible solutions. We can see that given a cycle of length 1 in *XY* we know:

$$X: 3 \to x \qquad Y: x \to 3$$

$$X: x \to 3 \qquad Y: 3 \to x$$

for some $x \in XY$.

We can see that $X = (3x)$ ... and $Y = (x3)$ ... which results in $XY = (3)(x)$ .... Therefore the cycles of length one in *XY* contain the same elements as a transposition in *X* and *Y*.

Now consider the possible transpositions in XY that result in the cycle (39) in the permutation $XY = (146)(258)(39)(70)$. From this example we can see that given a cycle of length 2 we have:

$$X: 3 \to x \qquad Y: x \to 9$$

$$X: x \to 3 \qquad Y: 9 \to x$$

$$X: 9 \to y \qquad Y: y \to 3$$

$$X: y \to 9 \qquad Y: 3 \to y$$

for some $x, y \in XY$.

We can see that $X = (3x)(9y)$ ... and $Y = (x9)(y3)$ ... which results in $XY = (39)(xy)$ .... Therefore the cycles of length two in *XY*, contain the same elements as transpositions in *X* and *Y*.

Next we will consider the cycles of length 3 in the permutation

$XY = (146)(258)(39)(70)$. We see:

$$X: 1 \to x \qquad Y: x \to 4$$

$$X: x \to 1 \qquad Y: 4 \to x$$

$$X: 4 \to y \qquad Y: y \to 6$$

$$X: y \to 4 \qquad Y: 6 \to y$$

$$X: 6 \to z \qquad Y: z \to 1$$

$$X: z \to 6 \qquad Y: 1 \to z$$

for some $x, y, z \in XY$.

We can see that $X = (1x)(4y)(6z)$ ... and $Y = (4x)(6y)(1z)$ ... which results in $XY = (146)(xzy)$. As we can see we have the inverse of (xyz). This result is why when using the method of writing one permutation under the other we use the inverse of the permutation that is written on the bottom.

Proof of Theorem 6.2: the above methods can be generalized as follows:

$$XY = (a_1 a_2 \dots a_{k-1} a_k)(b_1 b_2 \dots b_{k-1} b_k) \dots$$

$$X: a_1 \to x_1 \qquad Y: x_1 \to a_2$$

$$X: x_1 \to a_1 \qquad Y: a_2 \to x_1$$

$$X: a_2 \to x_2 \qquad Y: x_2 \to a_3$$

$$X: x_2 \to a_2 \qquad Y: a_3 \to x_2$$

$$\vdots \qquad\qquad \vdots$$

$$X: a_{k-1} \to x_{k-1} \qquad Y: x_{k-1} \to a_k$$

$$X: x_{k-1} \to a_{k-1} \qquad Y: a_k \to x_{k-1}$$

$$X: a_k \to x_k \qquad Y: x_k \to a_1$$

$$X: x_k \to a_k \qquad Y: a_1 \to x_k$$

for $x \in XY$,

we get $X = (a_1x_1)(a_2x_2) \dots (a_{k-1}x_{k-1})(a_kx_k)$ and $Y = (a_2x_1)(a_3x_2) \dots (a_kx_{k-1})(a_1x_k)$ resulting in the two cycles of length k, with $XY = (a_1a_2 \dots a_{k-1}a_k)\ (x_1x_kx_{k-1} \dots x_2)$ ..., where $(x_1x_kx_{k-1} \dots x_2) = (b_1b_2 \dots b_k)$. As we can see the order of the second cycle is again reversed. Therefore given the transposition(a_ix_j) in X, $(a_{i+1}b_{j-1})$ is also a transposition in X where a and b are elements of two different cycles of the same length.

From Theorem 6.2 it can be seen that the converse Theorem 6.1 is also true; that is:

THEOREM 6.3 Given a permutation consisting of an even number of disjoint cycles of each length, then this permutation can be written as a product of two permutations of the same degree, where each permutations consists only of disjoint transpositions.

The proof directly follows from the proof of Theorems 6.1 and 6.2 above. Given:

$AB=(a_1, a_3, \dots, a_{2k-3}, a_{2k-1})(a_{2k}, a_{2k-2}, \dots, a_4, a_2)(b_1, b_3, \dots, b_{2m-3}, b_{2m-1})(b_{2m}, b_{2m-2}, \dots, b_4, b_2)\dots$

$$A=(a_1, a_2)(a_3, a_4)\dots(a_{2k-1}, a_{2k})(b_1, b_2)(b_3, b_4)\dots(b_{2m-1}, b_{2m})\dots$$

$$B=(a_2, a_3)(a_4, a_5)\dots(a_{2k}, a_1)(b_2, b_3)(b_4, b_5)\dots(b_{2m}, b_1)\dots$$

Note that from Theorem 6.2 this is only one possible solution for A and B.

7 Luck, Math and Mistakes

Before we begin to discuss the methods used in decrypting messages, it is important to know some cryptanalysis definitions.

DEFINITION 7.1 **Plaintext** – the original message before encryption

DEFINITION 7.2 **Ciphertext** – the encrypted message

DEFINITION 7.3 **Key** - A sequence of symbols that controls the operation of a cryptographic transformation. For the Enigma, the key would be the initial rotor settings, plugboard settings and the positions of each of the three rotors.

When the Germans first began using Enigma to send encrypted messages, each operator would use the same key to encrypt and decrypt messages. However, it would be possible, given enough intercepted messages, for the enemy to deduce information about the machine using frequency analysis. Therefore, another method was adopted.[27] The Germans used a key book, distributed every couple of months, containing the initial rotor settings and plugboard settings to be used each day. When encoding a message the sender would now set their machine to the daily settings and then randomly choose their own 3-letter message key. The 3-letter message key they selected would then be encrypted twice using the daily key settings, and those six encrypted letters would be transcribed before the actual message. The message key was encrypted twice in order to make sure the recipient received the correct key, for it was still possible for the sender to make an error in encrypting his key. The sender would then set the three rotors in the machine to the message key that they selected and then encrypt the message. The recipient then sets their machine to the daily settings and decodes the six letter message key at the beginning of the message, which because of the reflector, will result in the sender's 3-letter message key written twice. The recipient then sets the rotors of their machine to the sender's key, and decodes the message. For example:

> Assume the daily rotor setting is `BLE` and the sender chooses `FMZ` as the message setting. The rotors are then set to `BLE` and using the keyboard `FMZFMZ` is encrypted to

[27] Singh p.148

LOCWHQ. The rotors are then set to FMZ and the plain text is encrypted. The cipher text is preceded by LOCWHQ and is sent to the recipient. The recipient sets the rotors of their machine to day key BLE and decodes LOCWHQ, which should result in FMZFMZ. The machine rotors are then set to FMZ and the cipher text is decoded.[28]

While this method implemented by the Germans made it so each message sent throughout the day was encrypted using a different key, this technique turned out to be the Achilles heel of the Enigma.[29]

Rejewski recognized that these six letter keys could be used to construct permutations, which would help lead to the determination of the wirings of each rotor. Given an arbitrary encrypted message key ABCDEF it is known that A and D were the result of pressing the same letter at different settings, as were B and E, and C and F. Knowing this we can construct permutations AD, BE and CF. It is important to note that the variables ABCDEF used to represent the message key are not the same as the variables used to represent the permutations AD, BE and CF. For example:

Given the intercepted message keys:

LOCWHQ WFQPRE PHEMFL

we can construct fragments of the permutations AD, BE, and CF. Again, since the message key was encrypted twice we know that in the key ABCDEF, A and D resulted from encrypting the same letter; similarly B and E, as well as C and F resulted from encrypting the same letter in each of the two cases. Using this knowledge we can construct the permutation AD, by considering the first and fourth letters in each encrypted key, so given the intercepted message

[28] Churchhouse p. 123
[29] Churchhouse p. 123

keys shown above, we can see L transforms to W, W to P and P to M, resulting in a fragment of AD equal to (LWPM...). Similarly, we get BE=(OHFR...) and CF=(CQEL...). In order to get the complete permutations of the entire alphabet, approximately sixty messages must be intercepted on a given day.[30]

Consider the following set of 56 intercepted keys:

LOCWHQ	WFQPRE	PHEMFL	ALORTS	ZFPERT	DQNDSF	TYUZIH	PLKMTJ
OZNOJF	RYLHIB	QYHNIZ	MNOVDS	WNMPDU	MLZVTA	EYTQIN	NJCTQQ
DNEDDL	CNSCDP	QPONVS	KIDIZX	NCITEM	NCKTEJ	UABKMO	PALMMB
NCWTEI	HGJAWC	NXCTPQ	PAKMMJ	DCIDEM	PSNMYF	LAMWMU	HHDAFX
PALMMB	OCJOEC	ISJUYC	XANYMF	MZKVJJ	OSNOYF	UDUKXH	IAOUMS
BBGBKW	VERLUG	EKVQBR	FMXJCV	GRYXLD	JTZSOA	YUFGAK	ZVEENL
AFXRRV	POFMHK	POAMHY	KALIMB	SPMFTU	EWSQGP	KWDIGX	GJIXQM

Figure 7.1

With these keys we can construct the complete permutations:

AD=(LWPMV)(TZEQN)(ARH)(KIU)(SFJ)(GXY)(B)(C)(O)(D)

BE=(OHFRLT)(QSYIZJ)(AMCEU)(NDXPV)(KB)(GW)

CF=(CQELBOSPTNFKJ)(UHZAYDXVRGWIM)

Note that each permutation *AD, BE* and *CF* are composed of an even number of disjoint cycles of the same length. From these products of permutations we can solve for possible solutions for each of *A* through *F,* which are the permutations produced by the machine at each of the first six settings. Recall that because of the reflector, each permutation *A* through *F* will be composed of disjoint transpositions. Consider the following product *AD*:

$$AD = (ADF)(BEH)(C)(G)$$

[30] Rejewski p. 218

We can find all possible solutions for *A* and *D* by using Theorem 6.3 and taking two of the cycles of the same length, placing the inverse of one underneath the other, and proceed to shift through all of the possibilities, as follows:

$\begin{pmatrix} ADF \\ HEB \end{pmatrix}$	$\begin{pmatrix} C \\ G \end{pmatrix}$
$\begin{pmatrix} ADF \\ EBH \end{pmatrix}$	$\begin{pmatrix} C \\ G \end{pmatrix}$
$\begin{pmatrix} ADF \\ BHE \end{pmatrix}$	$\begin{pmatrix} C \\ G \end{pmatrix}$

Figure 7.2

Our first row results in the permutation:

$$(AH)(DE)(FB)(CG)$$

The second row provides the permutation:

$$(AE)(DB)(FH)(CG)$$

And the third row gives the permutation:

$$(AB)(DH)(FE)(CG)$$

Therefore, from the permutations constructed by the message keys, we can solve for a relatively small number of possibilities for the permutations *A* through *F.* For example if *A* is the permutation that resulted from the third row in Figure 7.2, that is, *A*=(AB)(DH)(FE)(CG), then *D*=(BD)(HF)(AE)(CG), which is the permutation that resulted from row two in Figure 7.2. These permutations will be implemented later when the mathematics used to actually crack Enigma is discussed in more detail.

While the mistake made by the Germans of encrypting the message key twice was a vital element in helping to crack the Enigma, it was not the only thing that aided Rejewski in his work. The Allies received many lucky breaks over the years as they worked to crack Enigma,

thanks in most part to spies who collected a variety of information on the machine as well as information provided by Germans who committed treason.

Hans-Thilo Schmidt was born into a successful German family in 1888. He joined the German Army, but after fighting in World War I, cuts had to be made as a result of the Treaty of Versailles, and Schmidt was deemed not worthy enough to maintain his position in the army. In attempts to support his family, he tried to make a living as a businessman, but the post-war depression and hyperinflation made it nearly impossible to have a consistent income. He regretfully turned to successful older brother Rudolph, who after the war rose in the army ranks to chief of staff of the Signal Corps. It was actually Rudolph himself who sanctioned the use of the Enigma cipher. It was arranged for Hans-Thilo to work in Berlin at the Chiffrierstelle, the office in charge of Germany's encrypted communications. Chiffrierstelle was Enigma's command center, and was a top-secret department of the German military. Hans-Thilo left his family in Bavaria, where he could afford to support them, and moved to a far more expensive Berlin. Living impoverished and without his family, Hans-Thilo soon had had enough of working beneath his older, well-respected brother, and for a nation that did not appreciate his service. Therefore, he sought revenge and money by offering information to the Allies that could hurt his country and at the same time get back at his brother. On November 8, 1931 he met a French secret agent in Belgium and, in exchange for 10,000 marks, presented the agent with two documents, of which the agent took pictures. These documents were the instructions for using the Enigma, complete with a sample message both in plaintext and ciphertext. While these

documents did not contain information on the wirings of the rotors, they contained information needed to deduce those wirings.[31]

While the French were the ones who obtained the information, they had no real urgency or need to decipher messages after their successes from the previous war; thus attempts to crack the Enigma were short-lived. The Poles, however, had just re-established themselves as an independent state; which geographically happened to be located between the ambitious communist Russia and Germany, whose government was eager to regain their previously owned territory. Being in this precarious position, the Poles expressed interest in any information other countries had on Enigma. The French, who ten years earlier signed an agreement of military cooperation with the Poles, released the information obtained from Schmidt. Fear of invasion became the driving force behind cracking the Enigma. [32]

While the information obtained by Schmidt played a significant role in the decryption of Enigma, the intelligence recovered by French spies was equally, if not more important. Rejewski himself recognized General Gustav Bertrand, a spy for the French Army, for procuring material that "was the decisive factor in breaking the machine's secrets." Bertrand managed to acquire a copy of two tables of daily keys for September and October of 1932.[33] With these key books Rejewski was able to make significant progress in cracking the Enigma.

8 Cracking the Enigma

Rejewski's main attack in cracking the Enigma was based on determining the wirings of the rotors. To do so, he used theories of permutations because each component of the machine

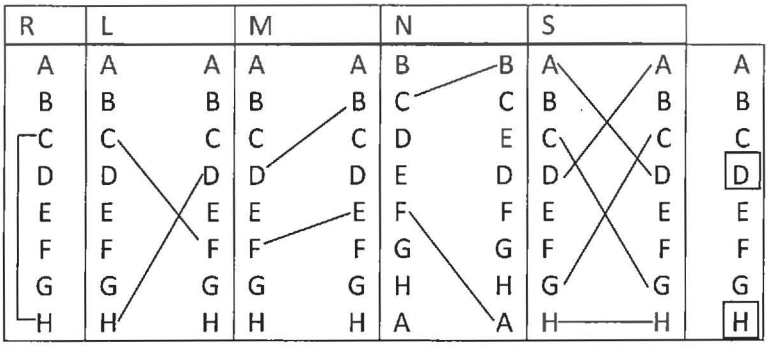
[31] Singh 145-146
[32] Singh pp.143-146
[33] Rejewski pp.219,221

was a different permutation of the alphabet. The composition of all of these permutations result in the permutation for a given setting, which is composed of 13 disjoint transpositions. Before we set up the equations we must first identify what each variable will represent.

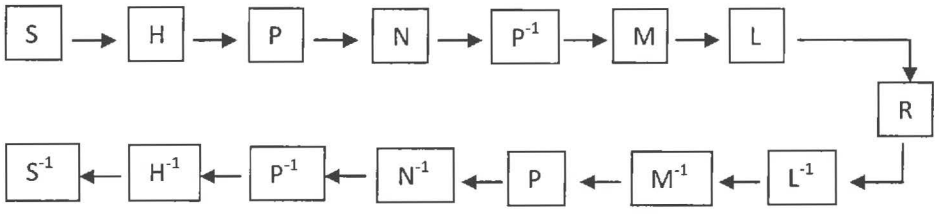
S – represents the permutation produced by the switchboard
L – represents the third and leftmost rotor
M – represents the second and middle rotor
N – represents the first and rightmost rotor
R – represents the reflector
H – represents the initial drum that connects the switchboard to the first rotor
P – represents the permutation of the alphabet to take into account the rotation of the rotors

The permutation $P = (abcdefghifklmnopqrstuvwxyz)$.

Using these variables we can represent our permutations *A* through *F,* the permutations found using the message keys on a given day. The equations for each permutation are obtained by simply following the current through the machine. Consider again our 8-letter Enigma from before:



As you follow the current through the machine you take the following path:



When a letter is pressed, the current first enters the switchboard *S*, then passes through the initial drum *H;* next, since the first rotor undergoes a rotation before the initial letter is encrypted, the letters are shifted by one letter in alphabetical order. Therefore, the conjugate of *N* by *P* is used to account for the initial rotation of *N.* Next, the current enters the middle rotor *M,* followed by the third rotor *L*. After it has passed through all three rotors, it enters the reflector, which then passes the current back through the rotors, switchboard and initial drum; therefore, these inverse permutations must be included in the equations. Therefore we arrive at the following equations:

$$A = SHPNP^{-1}MLRL^{-1}M^{-1}PN^{-1}P^{-1}H^{-1}S^{-1}$$
$$B = SHP^{2}NP^{-2}MLRL^{-1}M^{-1}P^{2}N^{-1}P^{-2}H^{-1}S^{-1}$$
$$C = SHP^{3}NP^{-3}MLRL^{-1}M^{-1}P^{3}N^{-1}P^{-3}H^{-1}S^{-1}$$
$$D = SHP^{4}NP^{-4}MLRL^{-1}M^{-1}P^{4}N^{-1}P^{-4}H^{-1}S^{-1}$$
$$E = SHP^{5}NP^{-5}MLRL^{-1}M^{-1}P^{5}N^{-1}P^{-5}H^{-1}S^{-1}$$
$$F = SHP^{6}NP^{-6}MLRL^{-1}M^{-1}P^{6}N^{-1}P^{-6}H^{-1}S^{-1}$$

These equations are written under the assumption that only the first rotor, *N,* rotates during the encoding of the first six letters, which is true in 21 of the 26 cases. It is true in 21 of the 26 cases because the setting on the first rotor that causes the second rotor to rotate will be reached at only 5 settings. Therefore, under this assumption we can treat the expression:

$$MLRL^{-1}M^{-1}$$

as a combined reflecting drum. Thus we denote this expression by the letter *Q*, which simplifies our equations to:

$$A = SHPNP^{-1}QPN^{-1}P^{-1}H^{-1}S^{-1}$$
$$B = SHP^{2}NP^{-2}QP^{2}N^{-1}P^{-2}H^{-1}S^{-1}$$
$$C = SHP^{3}NP^{-3}QP^{3}N^{-1}P^{-3}H^{-1}S^{-1}$$
$$D = SHP^{4}NP^{-4}QP^{4}N^{-1}P^{-4}H^{-1}S^{-1}$$

$$E = SHP^5NP^{-5}QP^5N^{-1}P^{-5}H^{-1}S^{-1}$$
$$F = SHP^6NP^{-6}QP^6N^{-1}P^{-6}H^{-1}S^{-1}$$

leaving us with a set of equations with four unknown permutations, *S, H, N* and *Q*.

At this point in time Rejewski struggled to solve for any of the unknown permutations. As the Cipher Bureau contemplated shutting down the operation, Rejewski continued his work with little success. However, on December 9th, 1932, at the most opportune moment, Rejewski was delivered the key books that General Bertrand had recovered. As a result of having the switchboard settings for two months, he could consider permutation *S* known. Therefore, the permutation *S* can be transformed to the other side of each equation as follows:

$$S^{-1}AS = HPNP^{-1}QPN^{-1}P^{-1}H^{-1}$$
$$S^{-1}BS = HP^2NP^{-2}QP^2N^{-1}P^{-2}H^{-1}$$
$$S^{-1}CS = HP^3NP^{-3}QP^3N^{-1}P^{-3}H^{-1}$$
$$S^{-1}DS = HP^4NP^{-4}QP^4N^{-1}P^{-4}H^{-1}$$
$$S^{-1}ES = HP^5NP^{-5}QP^5N^{-1}P^{-5}H^{-1}$$
$$S^{-1}FS = HP^6NP^{-6}QP^6N^{-1}P^{-6}H^{-1}$$

the left side consisting of known permutations. From previous work we have a small number of possible solutions for each *A* through *F*, so those permutations can be considered as known.

Rejewski had deduced that the initial drum was in fact the identity, a conclusion he arrived at by simply guessing, using the knowledge he had obtained from working with Enigma over the years. Therefore, our variable *H* is the identity and can be disregarded. Thus, we now have the set of equations:

$$SAS^{-1} = PNP^{-1}QPN^{-1}P^{-1}$$
$$SBS^{-1} = P^2NP^{-2}QP^2N^{-1}P^{-2}$$
$$SCS^{-1} = P^3NP^{-3}QP^3N^{-1}P^{-3}$$
$$SDS^{-1} = P^4NP^{-4}QP^4N^{-1}P^{-4}$$
$$SES^{-1} = P^5NP^{-5}QP^5N^{-1}P^{-5}$$
$$SFS^{-1} = P^6NP^{-6}QP^6N^{-1}P^{-6}$$

Since the permutation *P* is known, we can reduce the right side of the equation once more, resulting in the set of equations:

$$P^{-1}SAS^{-1}P = NP^{-1}QPN^{-1}$$
$$P^{-2}SBS^{-1}P^2 = NP^{-2}QP^2N^{-1}$$
$$P^{-3}SCS^{-1}P^3 = NP^{-3}QP^3N^{-1}$$
$$P^{-4}SDS^{-1}P^4 = NP^{-4}QP^4N^{-1}$$
$$P^{-5}SES^{-1}P^5 = NP^{-5}QP^5N^{-1}$$
$$P^{-6}SFS^{-1}P^6 = NP^{-6}QP^6N^{-1}$$

We will now represent each known, left side of the equations by a single variable, *U* through *Z*.

$$U = NP^{-1}QPN^{-1}$$
$$V = NP^{-2}QP^2N^{-1}$$
$$W = NP^{-3}QP^3N^{-1}$$
$$X = NP^{-4}QP^4N^{-1}$$
$$Y = NP^{-5}QP^5N^{-1}$$
$$Z = NP^{-6}QP^6N^{-1}$$

Now the products of each consecutive pair of *U* through *Z* will be taken:

$$UV = (NP^{-1}QPN^{-1})(NP^{-2}QP^2N^{-1})$$
$$VW = (NP^{-2}QP^2N^{-1})(NP^{-3}QP^3N^{-1})$$
$$WX = (NP^{-3}QP^3N^{-1})(NP^{-4}QP^4N^{-1})$$
$$XY = (NP^{-4}QP^4N^{-1}(NP^{-5}QP^5N^{-1})$$
$$YZ = (NP^{-5}QP^5N^{-1})\,(NP^{-6}QP^6N^{-1})$$

We can reduce these products to:

$$UV = NP^{-1}(QP^{-1}QP)PN^{-1}$$
$$VW = NP^{-2}(QP^{-1}QP)P^2N^{-1}$$
$$WX = NP^{-3}(QP^{-1}QP)P^3N^{-1}$$
$$XY = NP^{-4}(QP^{-1}QP)P^4N^{-1}$$
$$YZ = NP^{-5}(Q\,P^{-1}QP)P^5N^{-1}$$

We can now eliminate the common expression $QP^{-1}QP$ from each of the equations by solving for the expression and substituting in the equation of the product that precedes each equation. When solving for $QP^{-1}QP$ we get:

$$PN^{-1}(UV)NP^{-1} = (QP^{-1}QP)$$
$$P^2N^{-1}(VW)NP^{-2} = (QP^{-1}QP)$$
$$P^3N^{-1}(WX)NP^{-3} = (QP^{-1}QP)$$
$$P^4N^{-1}(XY)NP^{-4} = (QP^{-1}QP)$$

We then proceed by substituting the left side of each equation for $QP^{-1}QP$ into the equation directly following it; i.e. substituting the expression containing *UV* for $QP^{-1}QP$ in the equation for VW and so on, to get:

$$VW = NP^{-2}(PN^{-1}(UV)NP^{-1})P^2N^{-1}$$
$$WX = NP^{-3}(P^2N^{-1}(VW)NP^{-2})P^3N^{-1}$$
$$XY = NP^{-4}(P^3N^{-1}(WX)NP^{-3})P^4N^{-1}$$
$$YZ = NP^{-5}(P^4N^{-1}(XY)NP^{-4})P^5N^{-1}$$

These equations can now be reduced to:

$$VW = NP^{-1}N^{-1}(UV)NPN^{-1}$$
$$WX = NP^{-1}N^{-1}(VW)NPN^{-1}$$
$$XY = NP^{-1}N^{-1}(WX)NPN^{-1}$$
$$YZ = NP^{-1}N^{-1}(XY)NPN^{-1}$$

Our original set of six equations with four unknowns has now been reduced to four equations with one unknown, NPN^{-1}. We can find all possible solutions for each *UV* to *YZ* from the expressions for which we substituted the variables *U* through *X:*

$$U = P^{-1}SAS^{-1}P$$
$$V = P^{-2}SBS^{-1}P^2$$
$$W = P^{-3}SCS^{-1}P^3$$
$$X = P^{-4}SDS^{-1}P^4$$

These solutions can be found using the methods from Theorem 6.2. From here we proceed by writing out all possible permutations *UV* and *VW,* and compare the cycle structures of each of

the permutations found using the same *V* permutation. Since *UV* is a conjugate of *VW,* they must have the same cycle structure by Thereom 5.2. Once we have found all permutations *UV* and *VW* that have the same cycle structure for a given *V*, we proceed to solve for all permutations *WX*, using the same permutation *W* found in the corresponding *VW* permutation. Again ,because of Theorem 5.2, we are looking for permutations *WX* that have the same cycle structure as the *UV* and *VW* permutations previously found. Once all possible combinations of *U, V, W* and *X* have been found that provide the same cycle structures for each of the three products we have narrowed our possible solutions significantly. Using our possible combinations, the goal is to now solve for the unknown NPN^{-1}, by referring to the equations:

$$VW = NP^{-1}N^{-1}(UV)NPN^{-1}$$
$$WX = NP^{-1}N^{-1}(VW)NPN^{-1}$$
$$XY = NP^{-1}N^{-1}(WX)NPN^{-1}$$
$$YZ = NP^{-1}N^{-1}(XY)NPN^{-1}$$

By Corollary 5.1 we can proceed by choosing one of the possible *U, V, W* and *X* combinations and write all possible combinations of *VW* under *UV* and *WX* under *VW.* For example consider the following *U, V, W* and *X* permutations along with their corresponding *UV, VW,* and *WX* products:

UV=(adc)(beg)(fh) VW=(adh)(egf)(bc) WX=(adb)(cgf)(eh)

UV	(ADC)	(BEG)	(FH)	VW	(ADH)	(EGF)	(BC)
VW	(ADH)	(EGF)	(BC)	WX	(ADB)	(CGF)	(EH)
	(DHA)	(GFE)	(CB)		(DBA)	(GFC)	(HE)
	(HAD)	(FEG)			(BAD)	(FCG)	
	(EGF)	(ADH)			(CGF)	(ADB)	
	(GFE)	(DHA)			(GFC)	(DBA)	
	(FEG)	(HAD)			(FCG)	(BAD)	

Table 8.1

Reading as you would read permutation notation you can see that in writing *VW* under *UV* we see that *F* must permute to *B* or *C* and similarly *H* must permute to *B* or *C*. Therefore we can reduce our possibilities in writing *WX* under *VW* to:

UV	(ADC)	(BEG)	(FH)	VW	(ADH)	(EGF)	(BC)
VW	(ADH)	(EGF)	(BC)	WX	(ADB)	~~(CGF)~~	(EH)
	(DHA)	(GFE)	(CB)		~~(DBA)~~	(GFC)	(HE)
	(HAD)	(FEG)			~~(BAD)~~	~~(FCG)~~	
	(EGF)	(ADH)			~~(CGF)~~	(ADB)	
	(GFE)	(DHA)			(GFC)	~~(DBA)~~	
	(FEG)	(HAD)			~~(FCG)~~	~~(BAD)~~	

Table 8.2

Like before, when observing the permutations of *WX* under *VW*, it can be determined that *B* is permuted to either *H* or *E,* and *C* is permuted to the remaining *H* or *E.* Therefore, we can also reduce the left side of our chart as follows:

UV	(ADC)	(BEG)	(FH)	VW	(ADH)	(EGF)	(BC)
VW	(ADH)	(EGF)	(BC)	WX	(ADB)	~~(CGF)~~	(EH)
	~~(DHA)~~	~~(GFE)~~	(CB)		~~(DBA)~~	(GFC)	(HE)
	~~(HAD)~~	~~(FEG)~~			~~(BAD)~~	~~(FCG)~~	
	~~(EGF)~~	~~(ADH)~~			~~(CGF)~~	(ADB)	
	(GFE)	~~(DHA)~~			(GFC)	~~(DBA)~~	
	~~(FEG)~~	(HAD)			~~(FCG)~~	~~(BAD)~~	

Table 8.3

From here we are left with just two permutations that could possibly represent NPN^{-1}, but recall these permutations resulted from just one of our *U, V, W* and *X* combinations, so the same process as above must be applied to all combinations until the correct solution is found. Going back to our *Table 8.3* above, we have the two possible solutions for our unknown NPN^{-1}:

$$\begin{pmatrix} ADCBEGFH \\ ADHEGFCB \end{pmatrix} = (A)(D)(CHBEGF) \text{ and } \begin{pmatrix} ADCBEGFH \\ GFEHADBC \end{pmatrix} = (AGDFBHCE)$$

So:

$$NPN^{-1} = (A)(D)(CHBEGF) \text{ or } NPN^{-1} = (AGDFBHCE)$$

As you can see from these equations, NPN^{-1} is the result of P conjugated by N, therefore the solution must have the same cycle structure as P. The permutation P, is a permutation of the alphabet corresponding to one rotation of the rotor; thus $P = (ABCDEFGH)$. As written, P is composed of one cycle of length 8; therefore NPN^{-1} must be composed of one cycle of length 8. Thus from our two possible solutions found above, the correct permutation for NPN^{-1} is the 8 letter cycle: $(AGDFBHCE)$.

Now that we have found the solution to NPN^{-1} we can deduce the permutation N using a similar technique by using Corollary 5.1. We will proceed by writing the permutation P under NPN^{-1} in all possible ways as follows:

(AGDFBHCE)
(ABCDEFGH)
(BCDEFGHA)
(CDEFGHAB)
(DEFGHABC)
(EFGHABCD)
(FGHABCDE)
(GHABCDEF)
(HABCDEFG)

In our example we only have 8 possibilities; however for the complete alphabet we would have 26. At this point we proceed by checking each possible solution to determine which yields the correct result and we have determined the permutation N. Since we know the correct *U, V* and *W* we can check *N* by determining which possibility satisfies the equation:

$$VW = NP^{-1}N^{-1}(UV)NPN^{-1}$$

The wirings of drum *N* are now known, and since in the key books given to Rejewski the rotors change position between months, the same methods can be applied to solve for one of the other two rotors when it was in the first and rightmost position. Once the wirings of two of the rotors were known, it was not difficult for Rejewski to solve for the wirings of the third rotor and the reflector. He utilized the German instructions for using Enigma, obtained from Schmidt to simplify this process, for the instructions included an example of a message in plaintext as well as ciphertext. Thus, the Poles were able to construct their own form of the military Enigma with the proper wirings. While this result was significant in the cracking of Enigma, it was only the first step, because there were still thousands of keys that could be used to encrypt a message.

9 Rejewski's Catalog and Bombe

By the end of 1932 Rejewski was able to reconstruct the German military Enigma, and by January 1933 his former colleagues, Henry Zygalski and Jerzy Rozycki, were asked to help decipher messages. Although Zygalski and Rozycki were once again working on the Enigma, Rejewski remained in isolation to continue his work.

Rejewski first returned to his equations for solving for the rotor wirings to determine the settings of each rotor. He did so under the assumption that the permutation *S* for the plugboard settings was the identity, which we know it is not. For now we will operate under that assumption, as Rejewski did; therefore from our equations above we have:

$$A = PNP^{-1}QPN^{-1}P^{-1}$$
$$B = P^2NP^{-2}QP^2N^{-1}P^{-2}$$
$$C = P^3NP^{-3}QP^3N^{-1}P^{-3}$$
$$D = P^4NP^{-4}QP^4N^{-1}P^{-4}$$

$$E = P^5NP^{-5}QP^5N^{-1}P^{-5}$$
$$F = P^6NP^{-6}QP^6N^{-1}P^{-6}$$

We then solve for the permutation *Q*, which is equal to $MLRL^{-1}M^{-1}$, to get:

$$PN^{-1}P^{-1}APNP^{-1} = Q$$
$$P^2N^{-1}P^{-2}BP^2NP^{-2} = Q$$
$$P^3N^{-1}P^{-3}CP^3NP^{-3} = Q$$
$$P^4N^{-1}P^{-4}DP^4NP^{-4} = Q$$
$$P^5N^{-1}P^{-5}EP^5NP^{-5} = Q$$
$$P^6N^{-1}P^{-6}FP^6NP^{-6} = Q$$

However, while the permutation *N,* which if you recall is the wiring of the first rotor, is known, its setting is not. Therefore, we more correctly write these permutations as:

$$P^xN^{-1}P^{-x}AP^xNP^{-x} = Q$$
$$P^{x+1}N^{-1}P^{-x-1}BP^{x+1}NP^{-x-1} = Q$$
$$P^{x+2}N^{-1}P^{-x-2}CP^{x+2}NP^{-x-2} = Q$$
$$P^{x+3}N^{-1}P^{-x-3}DP^{x+3}NP^{-x-3} = Q$$
$$P^{x+4}N^{-1}P^{-x-4}EP^{x+4}NP^{-x-4} = Q$$
$$P^{x+5}N^{-1}P^{-x-5}FP^{x+5}NP^{-x-5} = Q$$

With these equations it would then be sufficient to substitute in the numbers one to twenty-six for x and see which value of x results in equivalent *Q* values for the six expressions. It is important to note the positive exponent for P will be less than or equal to 25; therefore, the sums and differences calculated in the exponents from the above equation must be equated modulo 26. However, it was previously assumed that the permutation S was the identity, which we know is not true, so the evaluated permutations for *Q* will not be identical, but they will be of the same cycle structure and will have several similar mappings. In order to find these similar *Q* permutations, Rejewski came up with a scheme which he called the grid method. For each of the three rotors and their known wirings he found the permutations, N,

PNP^{-1}, P^2NP^{-2}, ... , $P^{25}NP^{-25}$, N, ... P^4NP^{-4} and wrote each evenly spaced on a piece of paper as follows:

N	$kjpzydtiohxcsgubrnwfmveqla$
PNP^{-1}	$ioyxcshngwbrftaqmveludpkzj$
P^2NP^{-2}	$nxwbrgmfvaqeszpludktcojyih$
.	
.	
.	
$P^{25}NP^{-25}$	$ghijaksmdnlepwqnzbvcxfrtyuo$
.	
.	
P^4NP^{-4}	$uzpekdtyocqxnjsbiramhwgflv$

Rejewski then proceeded to write the permutations that were determined for *A* through *F*; recall each permutation *A* through *F* resulted from the products of the 13 disjoint transpositions at a given setting. The permutations are written in the matrix form we first used to write permutations, on a piece of paper with six slits as follows:

A	$\begin{pmatrix} abcdefghijklmnopqrstuvwxyz \\ srwivhnfdolkygjxbapzecqmu \end{pmatrix}$
.	
.	
.	
F	$\begin{pmatrix} abcdefghijklmnopqrstuvwxyz \\ wxofkduihzevqscymtnrglabpj \end{pmatrix}$

This paper he called the grid.[34] We read each permutation top to bottom, so for *A*, a→s, b→r, etc.

Once the two papers were complete with all the necessary permutations, Rejewski would slide the grid over the paper with the rotor permutations until he found the same letters

[34] Rejewski p. 222

being mapped by a specific letter in the permutations. For example, consider an eight letter Enigma with the following permutations and the boxes representing the slits in the paper:

	$\begin{pmatrix} abcdefgh \\ dfeacbhg \end{pmatrix}$
N	$behgafcd$

	$\begin{pmatrix} abcdefgh \\ gedcbhaf \end{pmatrix}$
P^1NP^{-1}	$dfeacbhg$

	$\begin{pmatrix} abcdefgh \\ bafghcde \end{pmatrix}$
P^2NP^{-2}	$gedcbhaf$

	$\begin{pmatrix} abcdefgh \\ fcbghade \end{pmatrix}$
P^3NP^{-3}	$bafghcde$

	$\begin{pmatrix} abcdefgh \\ cgaedhbf \end{pmatrix}$
P^4NP^{-4}	$fcbghade$

	$\begin{pmatrix} abcdefgh \\ ehgfadcb \end{pmatrix}$
P^5NP^{-5}	$cgaedhbf$

Figure 9.1

These permutations do not line up so the grid is slid down the paper to line up with the next set of the rotor permutations, which now gives us:

A	$\begin{pmatrix} abcdefgh \\ dfeacbhg \end{pmatrix}$
P^1NP^{-1}	$dfeacbhg$

B	$\begin{pmatrix} abcdefgh \\ gedcbhaf \end{pmatrix}$
P^2NP^{-2}	$gedcbhaf$

C	$\begin{pmatrix} abcdefgh \\ bafghcde \end{pmatrix}$
P^3NP^{-3}	$bafghcde$

D	$\begin{pmatrix} abcdefgh \\ fcbghade \end{pmatrix}$
P^4NP^{-4}	$fcbghade$

E	$\begin{pmatrix} abcdefgh \\ cgaedhbf \end{pmatrix}$
P^5NP^{-5}	$cgaedhbf$

F	$\begin{pmatrix} abcdefgh \\ ehgfadcb \end{pmatrix}$
P^6NP^{-6}	$ehgfadcb$

Figure 9.2

The permutations now line up and we can not only solve for *Q* with *x*=1, as we found, but we now know the setting of rotor *N*. This is a simplified version without a plugboard so all of the letters match up directly.

For the complete alphabet, when using this method on the 26-letter Enigma, we must use the grid method to find at what point all permutations *A* through *F* are lined up with rotor permutations where the permutations have multiple matched letters. And for each of the six sets of permutations the incorrect matching should involve the same swapped letters. This incorrect matching is the result of the plugboard. Therefore, using the grid method, Rejewski

could not only find the setting of each rotor *N*, but he could simultaneously find the pairing on the plugboard and thus find the permutation *S*.

For example consider the changes to Figure 9.2 above:

A	$\begin{pmatrix} abcdefgh \\ dfeacbhg \end{pmatrix}$
P^1NP^{-1}	$dceafbhg$

B	$\begin{pmatrix} abcdefgh \\ gedcbhaf \end{pmatrix}$
P^2NP^{-2}	$gedfbhac$

C	$\begin{pmatrix} abcdefgh \\ bafghcde \end{pmatrix}$
P^3NP^{-3}	$bacghfde$

D	$\begin{pmatrix} abcdefgh \\ fcbghade \end{pmatrix}$
P^4NP^{-4}	$cfbghade$

E	$\begin{pmatrix} abcdefgh \\ cgaedhbf \end{pmatrix}$
P^5NP^{-5}	$fgaedhbc$

F	$\begin{pmatrix} abcdefgh \\ ehgfadcb \end{pmatrix}$
P^6NP^{-6}	$ehgcadfb$

Figure 9.3

It is seen that in all of the compared permutations above, all of the letters match up except *f* and *c,* which tells us that in the plugboard there is a cable connecting *f* and *c*.

With the setting of rotor *N* and the permutation *S* known, all that is left is to find the settings of rotors *L* and *M*, the permutations which were replaced by *Q*. Therefore, we write our permutation *Q* similarly to how we did before:

$$Q = P^y M P^{-y} P^z L P^{-z} R P^z L P^{-z} P^y M P^{-y}$$

Unfortunately, Rejewski could not find a simple method for solving for the correct *y* and *z* and simply had to try each of the 26*26=676 possibilities. After he presented his findings to his superiors, Zygalski and Rozycki were allowed to work with him full-time from that point on. The three mathematicians worked on finding the daily-key every day for the next three years as there were no changes made to the Enigma cipher. The more they worked through the grid method, solving for 676 permutations a day, the more they found various patterns and shortcuts to minimize the amount of work they would have to do on a given day.

By 1935, the majority of the German military was using the Engima cipher and each military branch had their own daily keys. A quicker, more efficient way of finding the daily keys was necessary to keep up with the expanding use of Enigma.

Rejewski returned to the very beginning of his work with permutations that were produced from the message keys, *AD*, *BE* and *CF,* and examined the cycle structure of each permutation. He came to the realization that the three permutation structures produced by a specific key were close to unique. After having replica machines built with the newly found wirings, Rejewski proceeded to catalog the permutation cycle structures that resulted from each particular setting. Using our example above:

AD=(LWPMV)(TZEQN)(ARH)(KIU)(SFJ)(GXY)(B)(C)(O)(D)

BE=(OHFRLT)(QSYIZJ)(AMCEU)(NDXPV)(KB)(GW)

CF=(CQELBOSPTNFKJ)(UHZAYDXVRGWIM)

We can see that *AD* has a cycle structure of (4)(4)(3)(3)(3)(3)(1)(1)(1)(1), *BE* has (6)(6)(5)(5)(2)(2) and *CF* has (13)(13). While it seems tedious and a tremendous amount of work, Rejewski and his colleagues proceeded to find the cycle structure for each of the 105,456 settings. That

number is quite small when compared to the $1.05x10^{16}$ settings that Rejewski initially faced. It took just over a year to complete the entire catalog, but once it was complete, Rejewski was able to easily identify each daily-key after finding the permutations *AD*, *BE* and *CF*, and finding the corresponding daily key with the same cycle structure in the catalog. Remember, the key is changed daily, so this process had to be carried out each day before the Poles could begin to decode messages.

To help make this process easier, Rejewski, Zygalski and Rozycki designed a machine that would basically do the majority of the work for them. This device was known as a cyclometer and consisted of two sets of rotors; for these two sets of rotors, the *N* rotor in the second set would be set three letters off from the *N* rotor in the first set. The machine also had a display of 26 lamps with switches, and a power source. When the lamp of a letter was turned on, all of the other letters that belonged to the same cycle would light up.[35] So all they had to do was count the light bulbs that lit up. The three mathematicians used six card files, one for each ordering of rotors, to write out the cycle lengths for all possible settings. Once completed, it took a mere ten to fifteen minutes to solve for the daily key. Quite unfortunately, on November 2, 1937, the Germans replaced the reflectors in all of the machines with reflectors that had different wirings; therefore, all of their work had to be repeated after finding the wirings of the new reflector.[36]

Unbeknownst to Rejewski, all the work he had done over the past years was not entirely necessary at the time, for Schmidt had continued to provide information to the Allies, including the key books that were used during this time. However, the chief of the Cipher Bureau, Major

---

[35] Rejewski p. 225
[36] Rejewski p. 225

Gwido Langer, believed that withholding such information would allow Rejewski to become well associated with finding daily keys, in preparation for when the inevitable war came and they would no longer have access to the key books.[37]

The catalog played a significant role for the time being, but on September 15, 1938, the Germans made another change; this time not to the machine but to their method of sending the daily keys. A new way of solving for the daily key needed to be devised, and the idea came to Rejewski of constructing a machine that would simultaneously rotate through the various settings in order to find patterns among the keys. The device was dubbed the Bombe and consisted of six sets of drums.

A few months after this change was made at the end of 1938, the Germans then implemented two more rotors to bring the total number of rotors to five. For a given setting, three of the five rotors could now be chosen for enciphering a message. To make things even more complicated, a month later the number of cables that swapped letters on the plugboard was increased to ten. The increase in cables now swapped twenty letters as opposed to the previous twelve. While it appeared that Rejewski would again have to start from scratch, that was not the case, for there were various networks of the German military that utilized the Enigma. One in particular, the network of a party security staff known as the SD, implemented the new rotors and cables but did not change their method of sending the daily key. Therefore, the Poles were able to use the encoded messages from the SD to solve for the wirings of the two new rotors using the same methods used in finding the wirings of the initial three rotors.[38] Even with a complete replica of the updated Enigma in their possession, they could no longer

[37] Singh pp. 156-157
[38] Rejewski p. 227

use their previous methods of finding permutations from the message keys. With Poland on the brink of war, Langer would have been tempted to turn the key books over to Rejewski that he had been receiving from Schmidt, but just when the Poles could have used that information the most, Schmidt cut off all contact.[39]

With the new additions to the Enigma, the Bombe needed to include several more sets of drums. The machine that would be needed was well out of the Poles' budget, and they lacked the manpower necessary to process all of the information. They were also racing against time, knowing Germany would invade their country soon. The decision was made to share their secrets of the progress they had made on cracking Enigma. On July 25 and 26, 1939, the Polish intelligence agency met with representatives of France and Britain. At the meeting they shared all of the information they had obtained and provided the French and British intelligence officers with two Enigma replicas. The Allies were astonished with the progress that had been made, for they had given up on the machine long ago.[40]

10 World War II

On September 1, 1939, Poland was invaded by Germany, and after carefully destroying all of their work, Rejewski and the Cipher Bureau fled to Russia with the help of General Bertrand.[41] For the duration of the war Rejewski and his colleagues were continually on the run from the Germans, and were not able to make anymore contributions to their work on the Enigma. Unfortunately, Rejewski would be the only one who would return to their homeland at the end of the war. However, thanks to Rejewski's work, the British were able to take over his

[39] Singh p. 158
[40] Rejewski p. 228
[41] Rejewski p. 228

work at Bletchley Park. By 1940 the British had successfully rebuilt the Polish Bombe with the necessary improvements needed to account for the changes in the machine. The work and construction of the Bombe was led mostly by Alan Turing; and by 1943 the updated and advanced Bombe is said to be the first real electronic computer built in the world.[42]

As Singh states, "surprise is an invaluable weapon for a commander to have at his disposal."[43] With Britain able to know what the Germans were going to do before it happened they were at a considerable advantage. If they intercepted plans for an attack they could send reinforcements; if they heard of weaknesses shared amongst the German military the Allies could make offensive moves to take advantage of those weaknesses. With the work done at Bletchley Park the Allies were always one step ahead of the Germans; for example, when Germany invaded Norway and Denmark, the cryptanalysts provided a "detailed picture of German operations." And during the Battle of Britain, times and locations of Germany's planned bomb raids were provided to Britain intelligence so the proper precautions could be taken.[44]

As the Enigma continually evolved throughout the war the people at Bletchley Park continually developed new techniques to crack the code. With an array of "mathematicians, scientists, linguists, chess grandmasters and crossword addicts" the ciphers were studied with a variety of different minds.[45] Winston Churchill, one of Britain's senior military figures called the group at Bletchley Park, "the geese who laid golden eggs and never cackled".[46] Bletchley Park remained a secret throughout the remainder of the war and in fact was not exposed until the

---

[42] Rejewski p. 229
43 Singh p.162
[44] Singh pp.162-163
[45] Singh p.165
[46] Singh p.179

1970's. At this time those who made contributions towards cracking the Enigma were finally recognized, and since Rejewski had been not been a member of the groups at Bletchley Park it was then that he became aware of the impact of the contributions he made before the war.[47]

11 Conclusion

Marian Rejewski, "The conqueror of the German Enigma", lived a relatively quiet life after returning to Poland, where he died in 1978.[48] While he remained unrecognized for the majority of his life, when the news of his impact on the Allies' victory over Nazi Germany was released, films were made on Rejewski's life.[49] Rejewski's implementation of theories of permutations of disjoint cycles was what allowed the men and women at Bletchley Park to break ciphers throughout World War II. It will forever remain unknown what might have happened during the war if France and Britain did not have this crucial information from Poland. The ability to read intercepted messages sent amongst the German military put the Allies at a significant advantage and played a vital role in the Ally victory. And as an anonymous author claims, it was "the math that saved the world"[50].

---

[47] Singh pp. 188-189
[48] Kippenhahn p.182
[49] Kippenhahn p. 182
[50] Brian Young. "Cracking the Enigma Machine - Rejewski, Turing and the Math that Saved the World". www.slideshare.net. 2009.

12 References

Anderson, Marlow; Todd Feil. "A First Course in Abstract Algebra: Rings, Groups, and Fields". 2nd ed. Florida: Chapman and Hall Press. 2005.

Christensen, Chris. "Polish Mathematicians Finding Patterns in Enigma Messages". In *Mathematics Magazine*. Vol. 80, No. 4, October 2007.

Churchhouse, Robert. "Codes and Ciphers: Julius Caesar, the Enigma, and the Internet". New York: Cambridge University Press. 2002.

Fraleigh, John. "A First Course in Abstract Algebra". Massachusetts: Addison-Wesley Publishing Company. 1967.

Gallian, Joseph. "Contemporary Abstract Algebra". 5th ed. New York: Houghton Mifflin Company. 2002.

Kippenhahn, Rudolf. "Code Breaking: A History and Exploration". New York: The Overlook Press. 1999.

Lunde, Paul. "The Book of Codes: Understanding the World of Hidden Messages". California: University of California Press. 2009.

Rejewski, Marian. "How Polish Mathematicians Deciphered the Enigma". In *Annals of the History of Computing.* Vol. 3, Number 3, July 1981. Florida. 1981.

Singh, Simon. "The Code Book: The Evolution of Secrecy from Mary Queen of Scots to Quantum Cryptography". New York: Random House. 1999.

Young, Brian. "Cracking the Enigma Machine - Rejewski, Turing and the Math that Saved the World". www.slideshare.net. 2009.